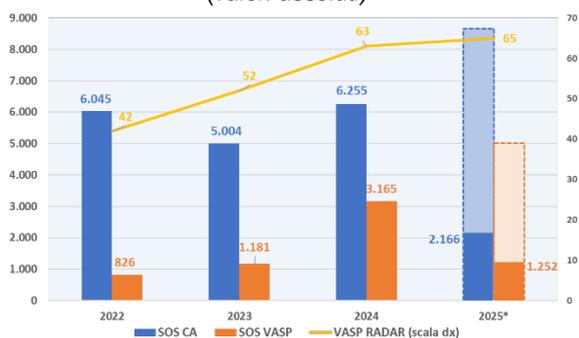


## SOS RELATIVE A CRIPTO-ATTIVITÀ

Dal 2024 le SOS relative all'uso di cripto-attività sono tornate a crescere grazie al contributo dei prestatori di servizi attivi nel comparto<sup>1</sup>. Nonostante alcune criticità, le informazioni ottenute dalla UIF mediante l'interazione diretta con tali operatori hanno consentito di svolgere analisi finanziarie su vari contesti sospetti.

Il trend di segnalazioni di operazioni sospette (SOS) riconducibili a cripto-attività (CA)<sup>2</sup> mostra un andamento positivo: nel 2024 sono pervenute 6.255 segnalazioni della specie, in aumento (+25%) rispetto al 2023; tale crescita è proseguita nel primo trimestre dell'anno in corso (2.166 SOS).

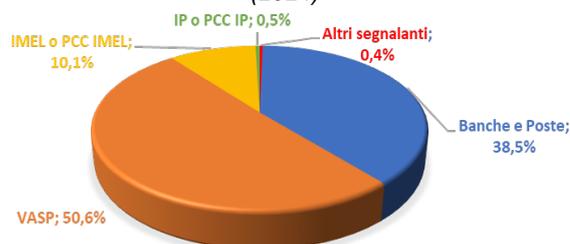
**SOS relative a cripto-attività**  
(valori assoluti)



L'aumento è dovuto all'incremento del flusso segnalativo dei VASP (+168% nel 2024), ascrivibile all'accresciuto numero di segnalanti attivi nel comparto che, per la prima volta, ha trasmesso la maggior parte delle SOS in argomento. Il contributo segnalativo del comparto tradizionale (principalmente banche e Poste, IMEL e IP e punti di contatto), invece, ha continuato a diminuire: già in calo nel 2023 (76,2%), nel 2024, la quota di SOS riferibile a CA inviata da tali

soggetti obbligati risulta di poco inferiore alla metà del totale (49,1%)<sup>3</sup> e ampiamente compensata da quella dei VASP, pari al 50,6% e cresciuta ulteriormente al 57,8% nel primo trimestre 2025.

**Distribuzione SOS CA per tipo segnalante**  
(2024)



Al 31 marzo 2025, risultano 65 VASP iscritti alla piattaforma RADAR; tuttavia, solo 30 operatori hanno trasmesso almeno una SOS dal 2024 e il flusso segnalativo risulta concentrato su pochi segnalanti.

Analogamente a quanto già registrato nel 2023, la maggior parte delle SOS in parola proviene da "VASP esteri" (86,8% nel 2024, 92,9% nel primo trimestre 2025) destinatari degli obblighi segnalativi alla UIF. Si tratta di operatori che, originariamente stabiliti all'estero, in virtù degli obblighi previsti dal regime di registrazione presso l'OAM, hanno costituito le loro sedi o stabili organizzazioni nel nostro paese.

La qualità delle SOS e delle ulteriori informazioni fornite dai VASP presenta in media profili di miglioramento, dovuti in parte alla non sempre solida conoscenza della normativa AML/CFT nazionale di alcuni VASP e a specifiche differenze culturali di quelli esteri<sup>4</sup>. La UIF si è quindi adoperata, anche tramite accessi ispettivi, per stimolare i VASP a innalzare il livello qualitativo delle informazioni trasmesse.

<sup>1</sup> Nella presente newsletter si utilizza per tali operatori la locuzione del GAFI *Virtual Asset Service Provider* (VASP), non essendo ancora operativo il regime autorizzativo previsto per i *Crypto Asset Service Provider* (CASP) introdotto dal Regolamento UE/2023/1114 relativo ai mercati delle cripto-attività (c.d. *Markets in Crypto-Assets Regulation* – MiCAR).

<sup>2</sup> SOS associate dai segnalanti o dalla UIF al fenomeno "Crypto Assets: Operatività Anomala" ovvero inviate da VASP.

<sup>3</sup> La diminuzione rilevata nel 2024 per i soggetti obbligati "tradizionali" (-19,2%), superiore al trend di calo generale rilevabile per le SOS ricevute dall'UIF (-3,3%), potrebbe ascrivere a una più accurata selezione dei contesti segnalativi nonché a una minor percezione di rischio associata ai *crypto-assets* indotta dal regime di registrazione dei VASP presso l'OAM.

<sup>4</sup> Diversi VASP esteri sono dotati di strutture AML/CFT costituite da personale straniero che non si è rivelato sempre adeguatamente formato rispetto alla normativa italiana e consapevole degli specifici fattori di rischio del nostro paese. Nei sistemi informatici e nei processi di selezione e trasmissione delle SOS di tali operatori si fa inoltre uso di lingue straniere, tipicamente l'inglese, che hanno reso più complesso rappresentare in italiano, in maniera corretta e completa, le operatività segnalate, nonché fornire le ulteriori informazioni richieste dall'Unità.

Nonostante tali criticità, la collaborazione attiva dei VASP ha consentito all'Unità di ricevere informazioni e svolgere analisi finanziarie approfondite sull'utilizzo di CA, sulla base di interazioni dirette della UIF con tali soggetti obbligati (cfr. *infra*).

#### **Dai VASP ai CASP: opportunità e sfide per la prevenzione ML/FT**

Il *framework* normativo recentemente innovato per effetto dei regolamenti MiCAR e TFR<sup>5</sup> e delle conseguenti disposizioni nazionali<sup>6</sup> offre, al contempo, opportunità e sfide per le attività AML/CFT. Tra le novità si segnalano: la disciplina della trasparenza dei trasferimenti di CA che coinvolgono almeno un CASP; l'introduzione di specifici regimi autorizzativi<sup>7</sup>; la qualificazione dei CASP come intermediari bancari e finanziari assoggettati a supervisione della [Banca d'Italia per i profili AML/CFT](#).

Inoltre, il c.d. "passaporto europeo" previsto dal MiCAR e l'applicazione delle disposizioni contenute nell'AMLR e nella AMLD<sup>8</sup> potrebbero determinare una rilevante rimodulazione del numero di CASP assoggettati a obblighi AML/CFT in Italia; occorrerà quindi attendere la conclusione del regime transitorio stabilito per le autorizzazioni dei CASP nell'Unione e l'attuazione delle richiamate previsioni anticirclaggio per valutare gli effetti che ne potranno derivare sui flussi segnaletici nonché sull'accessibilità diretta alle informazioni in possesso degli operatori del comparto, specie con riferimento ai CASP esteri che operano in Italia in regime di libera prestazione di servizi.

Nel 2024, tra le fattispecie più rilevanti in sede di analisi finanziaria sono emersi casi di:

- **Truffe**: l'acquisto di cripto-attività continua a essere realizzato spesso con fondi derivanti da varie tipologie di truffe (*romance scam*, *business email compromise*, nel campo del *trading online*, schemi fraudolenti di tipo piramidale, ecc.). Tali fenomenologie sono infatti presenti nel 36,4% delle SOS relative a CA; nel 42% considerando quelle trasmesse dai VASP;
- **VASP "compromessi"**: sono state riscontrate carenze nei presidi AML/CFT di alcuni VASP, tra cui l'assenza o l'incompletezza delle verifiche condotte sulla provenienza dei fondi ricevuti per conto dei loro clienti nonché sul profilo soggettivo di questi ultimi. In qualche caso, tali carenze sembrano ascrivibili a una compromissione degli stessi *provider* che, come confermato da indagini a loro carico, sono risultati coinvolti in schemi di riciclaggio ovvero in talune delle attività fraudolente sopra menzionate. Alcuni di questi operatori, non soggetti a regimi di vigilanza (cfr. *supra*) e che sfruttavano l'iscrizione in pubblici registri nazionali per dimostrarsi maggiormente affidabili, hanno causato ai propri clienti significative perdite pecuniarie;
- **Vulnerabilità dei "canali digitali"**: l'utilizzo di "canali digitali" per l'offerta al pubblico dei propri servizi da parte dei VASP (*app* per *smartphone* e *browser*) pone in luce sempre più spesso elementi di sospetto indicativi del possibile utilizzo dei *wallet* da parte di soggetti diversi dai legittimi titolari, rafforzando la percezione di maggiore anonimato in coloro che intendono attuare schemi di riciclaggio o altre attività illecite;
- **Darkweb e pedopornografia**: diverse SOS riguardano trasferimenti di CA, solitamente di importo contenuto, a favore di indirizzi riconducibili a piattaforme del *darkweb* attive nella vendita di prodotti illegali tra cui, talvolta, materiale pedopornografico.

Sempre più frequentemente le SOS riferiscono di operatività compiute con ricorso a *stablecoin*<sup>9</sup>, spesso ancorate al valore del dollaro americano, in luogo delle più tradizionali CA di tipo *unbacked* (come il BTC). Tali strumenti, tra l'altro disponibili in alcune applicazioni di messaggistica di ampia diffusione, consentono, in ragione della loro maggiore stabilità, di perfezionare trasferimenti di valore con tempi di validazione generalmente più contenuti dei bonifici e di più elevati livelli di anonimato mediante l'impiego di *wallet unhosted*<sup>10</sup>. Le *stablecoin*, utilizzate come forme "alternative" di pagamento, possono infatti concorrere ad alterare i "tradizionali" schemi di riciclaggio tramite CA, riducendo o in certi casi addirittura potenzialmente eliminando l'esigenza di convertire i flussi di origine criminale in valute ufficiali.

<sup>5</sup> Regolamento UE/2023/1113, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (c.d. *Transfers of Funds Regulation recast* - TFR).

<sup>6</sup> Cfr. il d.lgs. 129/2024 e il d.lgs. 204/2024 (quest'ultimo ha modificato il d.lgs. 231/2007).

<sup>7</sup> Le disposizioni in tema di riserva di attività sono presidiate da sanzioni penali.

<sup>8</sup> Si tratta, rispettivamente, del regolamento UE/2024/1624 (AMLR) e della direttiva UE/2024/1640 (AMLD6).

<sup>9</sup> Cripto-attività il cui valore si mantiene stabile facendo riferimento a valute ufficiali o *asset* tradizionali. Negli ultimi mesi le *stablecoin* sono state al centro dell'attenzione delle autorità e dei VASP europei, alla luce delle disposizioni del MiCAR a esse applicabili e relative agli *asset referenced token* (ART) e agli *e-money token* (EMT). Il 30 gennaio 2025, una [comunicazione congiunta Banca d'Italia – Consob](#) ha richiamato lo [statement dell'ESMA](#), con il quale tale Autorità ha ribadito il divieto di offerta al pubblico e di ammissione alla negoziazione di ART ed EMT emessi da soggetti non autorizzati ai sensi del predetto Regolamento europeo.

<sup>10</sup> Non gestiti da alcun VASP.